CHAPTER 11

Miscellaneous Administrative Tasks

This chapter describes various system maintenance and setup tasks you may need to perform. It covers these tasks:

Obtaining Version Information

Every ACE XML appliance has a version number that identifies the appliance's software with a particular release. This information is often required when contacting Cisco support or to ensure that all appliances in a cluster are running the same software version.

To obtain version information from the ACE XML appliance:

Step 1 Log into the appliance shell as the `root` user.

Step 2 In the **Main Menu**, choose the **Advanced Options** menu item.

The **Advanced Options** menu appears.

Step 3 Choose the **Version Information** menu item.

The release identifier string appears as a banner at the top of the screen. In the center of the screen, the appliance displays version numbers of the currently-installed Gateway software, operating system kernel, Tarari XML coprocessor card firmware (this option information refers to a hardware add-on option that is no longer available), and nForce hardware keystore card firmware.

Creating Appliance User Accounts

There are several types of user accounts in the system. Manager user accounts provide access to the ACE XML Manager web console interface.

Another type of user account is used for accessing the ACE XML appliance command-line environment. These accounts, called operating system accounts, enable access to terminal sessions on the appliance, whether locally using a console connected to the appliance or remotely using secure shell (SSH).

Each ACE XML appliance includes the built-in `root` account. The `root` user has broad privileges for performing operations on the ACE XML appliance. For security purposes, it is essential that access to the `root` account is controlled carefully. You can create additional login accounts to allocate limited administrative privileges to the appliance. User accounts also make it easier to audit configuration changes.

There are two types of user accounts for the appliance:

- Developer users access the appliance to install SDK extension
- Operator users access the appliance to roll and retrieve log files

Notice that the privileges in either case are very restrictive. For example, the menu-driven Shell interface is not available for either type of user. In both cases, they are restricted to the tasks listed.

To create a new login account on the ACE XML appliance:

Step 1 Log into the appliance shell as the `root` user.

Step 2 In the **Main Menu**, choose the **Advanced Options** item.

Step 3 Choose the **Run Bash** option on the **Advanced Options** page.

Step 4 At the `bash` prompt, create one of the two user types as follows:

- To create an operator user, enter the following command:

  ```
  reactivity-operator-add [username]
                  "[description]"
  ```

  where:

  - *[username]* is the login name of the new operator user.
  - *[description]* is a brief description of the account's purpose.

- To create a developer user, enter the following command:

  ```
  reactivity-developer-add [username]
                  "[description]"
  ```

  where:

  - *[username]* is the login name of the new user.
  - *[description]* is a brief description of the account.

Be sure to enclose the description with the double-quote character (") to ensure that the shell reads it correctly.

Step 5 Enter a password for the new account. When prompted, confirm the password by entering it again.

The new user can now log in to the shell interface.

Step 6 Type `exit` to return to the administration menu.

Backing Up and Restoring the System

Working policies are extremely valuable documents, often the result of many hours of planning and configuration. They also contain important and sensitive information about your network. You should treat them with the same care that you use with any other sensitive, mission-critical data, including having a backup and disaster recovery plan.

There are two approaches to backing up a system:

- By archiving individual policies and storing them offline. This captures policy changes made in the Manager interface, but excludes configuration settings made on the appliance directly.
- By backing up the state of the appliance with the backup command. This produces an archive file that contains the system state of the appliance, including configuration settings, policy, log files, and so on.

Most people will choose to do both, storing individual policies as needed, and maintaining a regular schedule of system backups. Archiving individual policies can be accomplished from the ACE XML Manager web console. (For instructions on doing so, see the chapter "Exporting a Policy to a File" in the *Cisco ACE XML Gateway User Guide*.) This section describes how to back up the entire system.

To back up a system or restore an appliance based on a previously saved backup, use the backup command on the appliance. The backup command is available on both Gateway systems and the Manager.

When you run the command, it examines the files on the appliance for any differences to the original state, excluding those that are runtime-process-oriented. This information is written to an archive file, which you can move to an appropriate storage medium for backup or recovery purposes.

Backing Up a System

The backup utility makes it possible to restore a system to a previously captured state. It saves the state of an appliance by recognizing changes that have been made to the system from its initial state and saving those changes to an archive. When that backup is restored on an appliance, the system is restored to the saved state.

Note Restoration from a backup file is intended to occur only on an ACE XML appliance with an empty configuration. Restoration may not work on an appliance that is not in that state.

System features saved by the backup utility include the policy state, the system's network configuration, and log information—essentially, any file created or modified since system installation, including scripts or data files.

There are some types of system changes or features that are not backed up by the backup/restore utility. For instance, it does not incorporate information that is specifically runtime-oriented, such as active process information. It also excludes certain types of system changes, such as software updates, hotfixes, or certified extensions installed by RPM. (Note that SDK extensions you have created and installed yourself *are* backed up.) You will need to restore these items separately, before using the backup and restore process.

The result of the backup operation is an archive file that contains new or changed files. Note that if you do not remove this archive file, it will be included in the next backup operation. It is therefore advised that after saving the backup file to a storage medium you remove the original from the appliance filesystem.

Before running the backup command, you should ensure that a sufficient amount of free space is available on the appliance for the backup process to work. The exact amount varies depending on the size of your policy, log files, and so on. In general, however, to back up everything except log files, you will need to have about 50 MB of free disk space on the appliance. If backing up event logs, audit logs, or traffic logs, you will need to have the amount of free disk space equal to the size of the logs. Therefore, if backing up the entire system, you will need 50MB plus the total size of the logs.

Note The backup operation does not itself check for sufficient disk space before starting. If the space is not available, the operation will not succeed.

To complete a backup, the backup utility does not stop ACE XML Gateway services that are running. Therefore, message traffic is not interrupted by this procedure.

To back up the system:

Step 1 Access the appliance shell on the ACE XML appliance you want to backup.

Step 2 Choose **Advanced Options > Run Bash**.

Step 3 Use the `backup` command to generate the backup file, as follows:

```
backup -all <filename>
```

Where filename is the name of the `tgz` file that will contain the backup archive. For example:

```
backup -all applianceBackup.tgz
```

The `-all` switch causes all data to be backed up, including network and Gateway configuration settings, the policy filestore, and log files. Alternatively, you can just specify a subset of the data to be backed up by using a command switch, such as:

```
backup -filestore applianceBackup.tgz
```

The *filestore* switch causes all data except log information to be backed up. To back up only log data, use either the `-userlog` (for the event log), `-auditlog`, or `-traffic` switches.

If you do not specify command options, only the network and Gateway configurations are backed up.

Note Enter `backup -h` to see all available options for the command. Notice the `-e` and `-l` switches. They cause command operation errors to be printed to standard error output. In general, you shouldn't have to use these options unless directed to do so by Cisco support.

After the process is finished creating the backup artifacts, you can use the scp (secure copy) utility to copy the archive to an off-box location. Generally, after copying the archive elsewhere, you should remove the backup archive from the appliance. If you do not, it will be included in the next backup archive you create.

Restoring a System

Restoration from a backup file is intended to occur only on an ACE XML appliance with an initial, empty configuration. Restoration may not work on an appliance that already contains a populated policy or that may have other changes from its initial state. It should, however, contain the same software version, hotfixes, and SDK extensions as the system used to generate the backup. These items should be separately installed before running the backup restore command.

Also, the appliance should be in the same operating mode as the system used to generate the backup file. That is, if the source system was configured in standalone mode, the target system should be configured for standalone mode as well.

After ensuring these prerequisites, restore the system as follows:

Step 1 Access the appliance shell on the ACE XML appliance on which you want restore the system.

Step 2 Choose **Advanced Options > Run Bash**.

Step 3 Use the `backup` script to restore the system from the backup file. The file should be either on the system or a disk location accessible from the appliance operating system.

For example:

```
backup -restore <filename>
```

Where filename is the name of the `tgz` file that was previously saved with the `backup` script. For example:

```
backup -restore -verbose applianceBackup.tgz
```

The `-verbose` switch enables error messages that occur during the backup or restoration process to be printed to the screen.

Note Enter `backup -h` to see a full list of options. To have errors in the operation printed to the screen, use the `-e` or `-l` switch.

Once you enter the command, the system reads the file and overwrites the current system with the appliance state represented in the file. After the changes are applied, the appliance reboots. After restarting, the system contains the state restored from the backup archive.

Step 4 If the hardware system of the target appliance is different from the source appliance, you will need to configure a license for the new appliance before it is fully operable. ACE XML Gateway licenses are bound to a particular machine, and therefore need to be separately acquired and installed for each physical appliance. For more information on acquiring and installing licenses, see "Configuring the Product License" section on page 5-27.

Applying an Update

Cisco occasionally issues updates to the ACE XML Gateway and Manager software. These updates typically include security enhancements, new features or feature enhancements, and bug fixes. Contact your Cisco support representative or check the Cisco support web site for information about software updates.

Each software update includes specific installation instructions tailored to that release. Because the specifics of upgrading may change from release to release, you should work with your Cisco support representative when performing any update.

In general, the update process consists of the following general steps:

1. Get the update files

   When an update for your software is available, you can obtain the needed files from Cisco support. In most cases the update package consists of an automated install package and installation instructions.

2. Read the update instructions thoroughly

   Be sure to read thoroughly the instructions that accompany the update package. The details of upgrading may vary from release to release, depending on the features affected by the update.

3. Prepare the update target appliance

   Before applying an update, it's a good idea to back up important files to ensure that you don't lose working policies, needed resources, or user accounts.

   You should perform such backups not only on the ACE XML Manager, but also on each ACE XML Gateway. See "Backing Up and Restoring the System" section on page 11-61 for details on backing up important files.

4. Apply the update to all ACE XML Gateway and Manager appliances. See the documentation that accompanies the update package for any special instructions.

If for any reason you need to restore your ACE XML Gateway instance to a previous version of its system software, use the instructions for performing such rollbacks included in software update distributions.

Configuring Serial Console Boot Control

By default, most ACE XML appliances are designed to support serial console access, with connection settings of 9600 bps, 8 data bits, no parity, and 1 stop bit.

By default, however, boot messages go to video console rather than to the serial console. You can change the configuration so that boot messages go to serial console as follows:

Step 1 Log in to the appliance shell as the `root` user.

Step 2 In the **Main Menu**, choose the **Advanced Options** item.

Step 3 Choose the **Boot Settings** item from the **Advanced Options**.

Step 4 Have boot output directed to serial console at startup by choosing the **Serial Port** item.

Note To use a keyboard, monitor, and mouse attached directly to the ACE XML appliance or through a KVM switch, choose the **Console** item.

The shell displays the **Advanced Options** screen. You must reboot the appliance to cause the new settings to take effect.

Step 5 From the **Advanced Options**, choose **Return to Main Menu**.

Step 6 From the **Main Menu**, choose the **Shutdown/Reboot** item.

Step 7 In the **Shutdown/Reboot** screen, choose **Reboot**.

Step 8 The shell prompts you to confirm your choice. Choose **Yes** to restart the appliance with the new settings.

When connecting a serial cable to the ACE XML appliance, be sure to connect it to the serial interface for the appliance and not for any cards that may be installed in the appliance.

The nCipher card shipped with ACE XML appliances has its own serial port, used only for nCipher card readers. It does not support terminal sessions.

Recovering from Low Disk Space

If the appliance shuts down unexpectedly, it could be due to lack of disk space. By default, log files are removed from disk usage exceeds a configured threshold. However, in certain cases, particularly if handling large message traffic, it's possible for the disk capacity to be reached.

The ACE XML Gateway and Manager are designed to shut down when available disk space is less than 10 percent of total disk space. If the appliance shuts down due to lack of disk space, you will need to free disk space on the affected appliance before it can be restarted.

If the ACE XML Manager shuts down due to a full disk, it will not subsequently start up completely until space is cleared. (This behavior prevents possible policy corruption errors due to lack of hard drive space.) If you attempt to start a Manager in this condition, the following message appears: "Starting ACE XML Manager: ACE XML Gateway console: detected full disk, cannot start"

Note The ACE XML Gateway shuts down if RAM memory use exceeds a given threshold as well. However, in this case the appliance recovers by itself.

To recover an appliance that has shut down due to lack of disk space:

Step 1 Connect to the appliance using SSH and log in as root user.

Note The appliance can continue to accept SSH connections even though disk space has caused other processes to shut down.

Step 2 From the **Main menu**, choose **Advanced Options > Run Bash**

Step 3 You can confirm that the disk space is low using the `df` command, which displays used and free disk space.

Step 4 Remove unneeded files from the disk. For more information about which files to remove, contact your Cisco support representative. If desired, first use `scp`, `cp`, or another copying tool to copy the files to another location prior to removal.

Step 5 Return to the menu by entering `exit` in the Bash shell and then select the appropriate menu option for returning to the Main menu.

Step 6 Restart the appliance by choosing one of the following from **Manage ACE XML Gateway Processes** menu:

- **Start ACE XML Gateway**
- **Start ACE XML Manager**

- **Restart All Configured Services** (if you choose this option with Gateways operating in your environment, the gateways are restarted, which may result in dropped network traffic.)

If you've encountered a full disk condition, you should check the settings that control automatic log file deletion. To do so, open the **ACE XML Gateway Settings** page in the Manager Web console, accessible from the **System Management** page. If appropriate, reduce the size threshold for the option labelled **Delete old log files when total message log disk usage exceeds**. Keep in mind that if this threshold is exceeded, the information in the deleted log files is lost. If it is important in your deployment to retain log information, you should use a script that automatically moves logs off disk at regular intervals.

For more information, see the online help available from the Manager.

Recovering System Passwords

The passwords for accessing the administration interfaces in the ACE XML Gateway system can be reset when needed. The following procedures describe how to reset the password for appliance console access and for ACE XML Manager web console access.

Console Access Password

The console interface of the ACE XML appliance is used to configure the appliance's initial operating and network settings. User accounts for console interface access include the built-in user account `root` along with custom accounts created through the `reactivity-operator-add` procedure.

The steps for resetting passwords for these two types vary as follows.

Resetting the Password for a Custom User Account

Passwords for custom-created user accounts (created by the reactivity-operator-add operation) can be reset by the `root` user using the `sudo passwd` command. That is, from the bash shell on the appliance, `root` user can change the password for a user account as follows:

sudo psswd <username>

After entering this command, you are prompted to enter a password for the user.

The command must be run from the bash shell of each appliance that the user needs to access.

Resetting the Password for the root User Account

Resetting the root user account password requires physical access to the appliance. Also, it requires you to shut down the appliance, constituting an interruption of service.

Before starting, connect a console to the appliance by serial or video connection.

Step 1 From the console, initiate a reboot of the system if possible (using the CTRL-ALT-DEL key sequence). If this is not possible, power cycle the appliance directly.

Note It is important to consider that power cycling an active appliance can in rare instances result in data corruption. Before performing this operation, it is suggested that you backup the appliance.

Step 2 As the appliance reboots, watch for the GRUB message “GRUB Loading Stage 2". Press the escape key immediately when it appears.

If you get a display with a box and instructions at the bottom, proceed. Otherwise repeat the reboot process.

Step 3 Enter commands using the following key sequences:

a. Enter “e” to edit the record.

b. Move the cursor to the “kernel” line using the arrow keys.

c. Enter “e” to edit the kernel line.

d. Enter a space followed by the number 1 (that is, “ 1”) to append the number 1 to the end of the line.

e. Press <enter> to accept the changes.

f. Enter “b” to boot with the modified configuration and wait for a shell prompt.

g. If asked to press "Y" to verify disk, it is recommended that you do so. The process will take extra time.

h. At the shell prompt, change the root password using the `passwd` command.

i. After entering the new password, reboot to normal operations with the “`reboot`” command.

After the system restarts, you can log in as the root user with the new password.

Resetting the Manager Web Console Password

In the ACE Manager web console, the password for custom-created user accounts can be changed at any time by the administrator user. The administrator does so by editing the user account in the User Administration pages. Changing the password for the built-in administrator account, however, requires the steps described in the following procedure.

Note The following steps do not apply for Manager user accounts verified by external LDAP or RADIUS systems. If using LDAP or RADIUS authorization modes, the password will need to be reset using the external system.

Keep in mind that a distinct administrator account exists for each cluster administered by the ACE XML Manager. When resetting the administrator password for an ACE XML Manager instance that administers multiple clusters, you will need to know the cluster in which t he password needs to be reset.

Step 1 Before starting, shut down the ACE XML Manager from the appliance console menu. (From the Main Menu, choose **Manage ACE XML Gateway Processes**, and then **Stop ACE XML Manager**.)

Step 2 Access the bash shell on the Manager appliance and locate the filestore for the cluster that needs resetting. The filestore can be found in:

- In versions 5.0.x and earlier, this is /usr/local/reactivity/console_documents/filestore

- In versions 5.1 and later, this is /var/lib/reactivity/console_documents/cluster<cluster_id>/filestore

  Where <cluster_id> is a unique string that identifies the cluster internally.

Note For information on determining the cluster ID, see "Understanding Configuration Data" section on page 13-89.

Replace the contents of the file `00/00/000000000003.00000000` with the text below.

```
<object type="user">
 <AccessControlRole>true</AccessControlRole>
 <ActiveGroupID>
  <ID>0000000000000004</ID>
 </ActiveGroupID>
 <ConsoleAdminRole>true</ConsoleAdminRole>
 <ExternalDeveloperRole>true</ExternalDeveloperRole>
 <FailedLoginCount>0</FailedLoginCount>
 <HashedPassword>mcVyzSCfpKjxx4W9KugFFPYPSB8=</HashedPassword>
 <IsDisabled>false</IsDisabled>
 <IsOperator>true</IsOperator>
 <MessageTrafficLogRole>true</MessageTrafficLogRole>
 <OperationsRole>true</OperationsRole>
 <PolicyViewRole>true</PolicyViewRole>
 <RoutingRole>true</RoutingRole>
 <Username>administrator</Username>
</object>
```

This resets the administrator password to the factory default.

Step 3 Start up the ACE XML Manager process.

Step 4 Log in to the web console as user `administrator` with password `swordfish`. Be sure to change the administrator password from the factory default after logging in.

Changing the MTA Postmaster Address

The ACE XML Gateway can receive SMTP traffic for certain types of services. Specifically, it can process and validate ebXML content passed as email attachments. To use ebXML service processing at the gateway, you configure an ebXML-based service definition in the Manager web console.

Note The Gateway's SMTP server never acts as a relay. It accepts incoming messages only for local addresses and it accepts outgoing messages only from the gateway. Periodically, the SMTP server attempts to resend messages that suffered transient failures. The MTA does not support SMTP over SSL or TLS within SMTP.

If an ebXML service is added to the policy, the appliance opens port 25 to handle SMTP traffic. Thereafter, it's possible for the ACE XML Gateway MTA to receive email in its postmaster mailbox.

The postmaster address is a standard administrative address for MTA's (as required by the SMTP protocol). It does not affect incoming or outgoing gateway traffic.

If desired, you can modify the address so that mail to the postmaster is sent to another location, or keep the default, in which case the postmaster mailbox is the root user's mailbox on the ACE XML Gateway.

To change the existing address:

Step 1 Log in to the shell interface of the gateway appliance as the `root` user.

Step 2 In the **Main Menu**, choose the **Advanced Options** item.

Step 3 In the **Advanced Options**, choose **MTA Configuration**.

Step 4 Choose the Configure postmaster address item.

Step 5 Enter the email address to which administrative information should be addressed.

Step 6 When finished, you can return to the **Advanced Options** menu from the **MTA Menu**.

Repeat these steps for each Gateway in the cluster.